REMARKS

Claims 1, 3-18, 20-29 and 31-33 are currently pending in the subject application and are presently under consideration.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments herein.

I. Rejection of Claims 1, 3-9, 17, 18, 20, 23 and 29 Under 35 U.S.C. §103(a)

Claims 1, 3-9, 17, 18, 20, 23 and 29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al.* ("A secure electronic software distribution (ESD) protocol based on PKC" by Lee *et al.*, EC-Web 2000, LNCS 1875, pp. 63-71, 2000), in view of Hypponen (U.S. 6,986,050 B2), and further in view of Bathrick *et al.* (U.S. 5,825,300). Wihtdrawal of this rejection is requested for the following reasons. Lee *et al,* Hyppopen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

> To reject claims in an application under §103, an examiner must show an unrebutted *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. This is achieved by providing a strong set of security credentials between a master entity such as a service and a remote entity such as a partner. In conjunction with the strong set of security credentials, a protocol is provided that acts as a package, wrapper or container to house the security credentials before delivery from the service to the partner to facilitate secure communications between the

parties. In particular, independent claim 1 recites *a system and method for facilitating a computer a security connection between entities, comprising* ***a wrapper that packages credentials associated with resources of a service; and a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key****, the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials*. Lee *et al.*, Hypponen and Bathrick, individually or in combination, fail to teach or suggest such aspects of the claimed invention.

Lee *et al.* discloses a secure electronic software distribution protocol based on public key cryptography (PKC). At page 5 of the Final Office Action, the Examiner contends that Lee *et al.* teaches a wrapper that packages credentials associated with resources of a service. Applicants' representative disagrees. In accordance with the claimed invention, the credentials packaged in the wrapper are those credentials employed by the service as proof that the holder should be granted access to the resources. On the contrary, Lee *et al.* packages software in the wrapper, the software being the resource offered to the customer. Thus Lee *et al.* is silent regarding ***a wrapper that packages credentials associated with resources of a service*** as recited by the subject claims.

At page 5 of the Final Office Action, the Examiner concedes that Lee *et al.* does not teach a pass phrase employed in connection with generation of cryptographic wrapping keys, the pass phrase distributed separately from the credentials. The Examiner attempts to compensate for the aforementioned deficiencies of Lee *et al.* with Hypponen and Bathrick *et al.* Hypponen discloses a method of securing data stored in an electronic device comprising encrypting the data using a cryptographic key. A user is asked to enter a password and a passphrase, the system uses the passphrase to generate a cryptographic key, stores it in the system and uses it to encrypt and decrypt the data. The passphrase taught by Hypponen is used to generate a cryptographic key that allows access to encrypted data. On the contrary, the cryptographic wrapping key generated from the pass-phase of applicants' claimed invention is employed in generating the wrapper. Thus, Hypponen is silent regarding ***a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key*** as recited by the subject claims.

Bathrick *et al.* teaches computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the

certification authority's domain. The certifying authority generates keying material, which includes a password and sends it to the subject entity via manual courier or other means that is different from the communication system operating through a network. Nowhere does Bathrick *et al*. teach ***a wrapper that packages credentials associated with resources of a service, a pass phrase employed in connection with generation of the wrapper via a cryptographic wrapping key*** as taught by applicants' subject claims.

Independent claim 18 recites *generating a strong password, generating a pass-phrase,* ***wrapping the password cryptographically via the pass-phrase****, storing the wrapped password in an executable, and* ***transmitting the executable and the pass-phrase to a system via different communications mediums***. At page 7 of the Final Office Action, the Examiner contends that Lee *et al*. teaches wrapping the password cryptographically via the pass-phrase. Applicants' representative disagrees. At the cited portions, the cited reference teaches an electronic license package where the cryptographic function H that cryptographically locks the password and the passphrase (secret string) together. Thus, Lee *et al*. is silent regarding *wrapping the password cryptographically* ***via the pass-phrase*** as recited by the subject claims.

Independent claim 28 recites *a first data packet comprising a password component employed to establish a trust relationship between at least two nodes and* ***a wrapper field employed to encapsulate the password,*** *the wrapper field mediating access to the password and a second data packet comprising* ***a pass-phrase employed to generate and unlock the wrapper field,*** *the pass-phrase distributed separately from the wrapper field*. Lee *et al*. fails to teach or suggest such aspects of the claimed invention.

At page 13 of the Final Office Action, the Examiner contends that Lee *et al*. teaches ***a wrapper field employed to encapsulate the password,*** *the wrapper field mediating access to the password and a second data packet comprising* ***a pass-phrase employed to generate and unlock the wrapper field.*** At the cited portions, the cited document teaches a cryptographic function H that cryptographically wraps the password, and a pass phrase that unlocks a different wrapper field, namely the one that packages the downloaded software. Thus, Lee *et al*. is silent regarding ***a wrapper field employed to encapsulate the password,*** *the wrapper field mediating access to the password and a second data packet comprising* ***a pass-phrase employed to generate and unlock the wrapper field*** as recited by the subject claims.

In view of the above, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 1, 18 and 28 (which claims 3-9, 17, 20, 23 and 29 depend respectively there from).

II. Rejection of Claims 10-12 Under 35 U.S.C. §103(a)

Claims 10-12 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al*., in view of Hypponen, in view of Bathrick *et al*., and further in view of Brainard (SecurSight: An architecture for secure information access, RSA Lab). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Claims 10-12 depend from independent claim 1. As discussed *supra*, Lee *et al.,* Hypponen and Bathrick *et al*., individually or in combination, do not teach or suggest each and every element set forth in the subject claim. In particular, Brainard does not make up for the deficiencies of Lee *et al,* Hypponen and Bathrick *et al*. with respect to independent claim 1 (from which claims 10-12 depend). Thus, it is respectfully submitted that this rejection be withdrawn.

III. Rejection of Claims 27, 28, 31 and 33 Under 35 U.S.C. §103(a)

Claims 27, 28, 31 and 33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al.*, in view of Bathrick *et al*. It is respectfully submitted that this rejection should be withdrawn for the following reasons. Lee *et al.*, and Bathrick, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

Independent claims 27, 28, 31and 33 recite similar limitations namely, *a computer-readable medium having stored thereon a signal to communicate security data between at least two nodes, comprising a first data packet comprising a password component employed to establish a trust relationship between at least two nodes* ***and a wrapper field employed to encapsulate the password****, the wrapper field mediating access to the password and a second data packet containing* ***a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field.*** Lee *et al*. and Bathrick *et al*. are silent about such novel aspects of the applicants' subject claims.

As discussed *supra*, Lee *et al*. does not disclose or suggest utilizing a pass-phrase to generate a wrapper and transmit the wrapper field separately from the pass-phrase. Bathrick *et al*. does not make up for the aforementioned deficiencies of Lee *et al*. Therefore, Lee *et al*. and Bathrick *et al*. individually or in combination do not teach ***a wrapper field employed to encapsulate the password, a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field*** as recited by applicants' subject claims. Accordingly, withdrawal of this rejection is requested.

IV. Rejection of Claims 13-16, 21, 22, 24, 25 and 32 Under 35 U.S.C. §103(a)

Claims 13-16, 21, 22, 24, 25 and 32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al.*, in view of Hypponen, and further in view of Bathrick *et al.* and Brainard. It is respectfully submitted that this rejection should be withdrawn for the following reasons. Lee *et al.*, Hypponen, Bathrick *et al*. and Brainard, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Brainard does not make up for the aforementioned deficiencies of Lee *et al.* and Bathrick *et al*. with respect to independent claims 1, 18 and 31 (which claims 13-16, 21-22, 24-25 and 32 depend from). Accordingly, withdrawal of this rejection is requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP319US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731